REMARKS

I. Status of the Claims:

Claims 1, 2, 6, 7, 8, 12, 13, 14, 16, 18-22, 25, 26-37, 39-53 are currently pending in the application. All claims are rejected. No new matter is introduced by this amendment. Accordingly, entry of this Amendment is respectfully requested.

II. Claim Rejections under 35 U.S.C. § 103:

Claims 1, 2, 6, 7, 8, 12, 13, 14, 16, 18-22, 25, 26-37, 39-53 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Fraser et al (US 5,835,595) in view of Wiser et al (US 6,385,596).

III. Applicant's Response

Claims 1, 2, 6, 7, 8, 12, 13, 14, 16, 18-22, 25, 26-37, 39-53 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Fraser et al (US 5,835,595) in view of Wiser et al (US 6,385,596).

The Examiner's rationale for combining Fraser with Wiser on page 3 of the Office action, reads as follows:

> Fraser discloses a method of processing information in a communications device, comprising: receiving from a first remote device content encrypted with a content key (e.g. col. 5 Ln 1-4); transmitting a request for the content key to a second remote device, the second remote device authorized to act on behalf of a provider of the content (e.g. col. 5 Ln 15-20).
>
> Fraser does not teach, but Wiser does receiving from the second remote device an encrypted version of the content key, wherein the encrypted version of the content key is encrypted with a public key of the communications device (e.g. col. 4 Ln 34-36); and decrypting the encrypted version of the content key with a private key of the communications device, the private key of the communications device corresponding to the public key of the communications device. (e.g. col. 4 Ln 10-40).

In response, in the Applicant's claimed invention a content distributor 104 is enabled to superdistribute content encrypted with a content key "K" to any recipient device. Any device may receive the encrypted content, but it may not make use of it without the content key. The content key is separately protected by further encrypting it with the public key of a device 106 that is the agent of the content distributor 104.

The Applicant's claimed invention enables any client 108 possessing an encrypted copy of the content, to superdistribute that encrypted content to a second client 110, without needing to request a second download of the encrypted content from the content distributor 104. The Applicant's claimed invention provides that when the content encrypted under the content key is distributed, the content key is also distributed in a form encrypted under the public key of the authorized agent 106. Thus, the claimed invention enables the encrypted security of the content to be maintained when it is received by a second client 110, because the content, which is encrypted under the content key, is distributed with the content key encrypted under the authorized agent's 106 public key. The second client 110 receives the content key encrypted under the authorized agent's 106 public key. The second client 110 then transmits a request for the content key to the authorized agent 106 of the content distributor 104, and the agent re-encrypts the content key under the requester's 110 public key and returns it to the requester 110.

The Applicant's claimed invention overcomes a significant problem confronting the system disclosed in the Wiser reference, namely the network bottleneck created at Wiser's content manager 112 by satisfying the requests for the content from many clients 126. Wiser's content manager 112 stores the content encrypted under the media key and a copy of the media key encrypted under the content manager's public key. In Wiser, every client 126 that wants a copy of the content must request it from the content manager, which re-encrypts the media key under the public key of the requesting client 126 and then downloads it and the encrypted content to the requester.

The Applicant is claiming a first occurring step of "(a) receiving from a first remote device superdistributed content encrypted with a content key."

This is followed by a second occurring step of: "(b) transmitting a request for the content key to a second remote device, the second remote device authorized to act on behalf of a provider of the content; said second remote device receiving the content key encrypted with a public key of the second remote device."

In contrast, Wiser at column 19, lines 15 to 60, reads in part, as follows:

> If the voucher ID is verified, the content manager 112 encrypts 954 the song's media key with the public key of the media player 116. In this manner, the media becomes specifically and individually licensed to the consumer; the media data file 200 is now referred to as the licensed media. ....
>
> The content manager 112 then returns 956 the encrypted media key ... to the delivery server 118.

> The delivery server 118 retrieves 958 the licensed media ... and sends 960 it to the media player 116 ....
>
> When a received media data file 200 is to be played back 964 .... The media player 116 then decrypts the media key with the consumer's private key 412. Finally, the media key is then used to decrypt the audio image 208 in real-time as the media is played.

Note the network bottleneck created at Wiser's content manager 112 by satisfying the requests for the content from many clients 126. Wiser's content manager 112 stores the content encrypted under the media key and a copy of the media key encrypted under the content manager's public key. In Wiser, every client 126 that wants a copy of the content must request it from the content manager, which re-encrypts the media key under the public key of the requesting client 126 and then downloads it and the encrypted content to the requester.

The Applicant's claimed invention overcomes the Wiser bottleneck by its superdistributed content encrypted with a content key, so that the content does not have to be obtained from a single source, such as Wiser's content manager 112.

The Wiser fails to disclose or suggest the Applicant's claimed invention.

Fraser does not disclose or suggest the Applicant's claimed invention, wherein the authorized agent has its own public key and private key and wherein the content key transmitted to the authorized agent is encrypted with the public key of the authorized agent. Instead, Fraser discloses at column 5, lines 16-20 that in step 309 of Fig. 3B, the content key λ_T is encrypted with the symmetric key encrypting key ρ, column 5, lines 16-20 reading as follows:

> ...certification module CM encrypts the secret key for the music title λ_T using the personality module's secret key ρ to obtain $\rho(\lambda_T)$. The encrypted secret key $\rho(\lambda_T)$ and the encrypted music $\lambda_T(T)$ are transferred to database 14 of the personality module at step 309...

Then Fraser discloses at column 5, lines 26-28 that in step 310 of Fig. 3B, the content key λ_T is decrypted with the symmetric key encrypting key ρ to obtain the content key λ_T, column 5, lines 26-28 reading as follows:

> At step 310, the personality module uses secret key ρ to decrypt λ_T. Module PM then uses λ_T to decrypt $\lambda_T(T)$ to extract music piece T.

Thus, Fraser does not disclose or suggest the Applicant's claimed invention, wherein the authorized agent has its own public key and private key and wherein the content key transmitted to the authorized agent is encrypted with the public key of the authorized agent.

The combination of Fraser with Wiser fails to disclose or suggest the Applicant's claimed invention, as discussed above. The Applicant's claims are patentable over the combination of Fraser with Wiser.

AUTHORIZATION

The Response is timely filed. Thus, no fee is due by filing of this paper. However, the Commissioner is authorized to charge any additional fees which may be required for timely consideration of this response, or credit any overpayment to Deposit Account No. 13-4500, Order No. 4208-4143.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Dated: December 13, 2007 By: _____

John E. Hoel
Registration No. 26,279
(202) 857-7887 Telephone
(202) 857-7929 Facsimile

Correspondence Address:
Morgan & Finnegan, L.L.P.
3 World Financial Center
New York, NY 10281-2101